IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Adam R. Schran		:	
Conf. No.:	3079	:	Group Art Unit: 2161
Appln. No.:	09/820,054	:	Examiner: Etienne Pierre Leroux
Filing Date:	March 28, 2001	:	Attorney Docket No.: 10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA	:	

TRANSMITTAL OF APPEAL BRIEF
(37 C.F.R. § 41.37)

Transmitted herewith is the Appeal Brief in this application, with respect to the concurrently filed Notice of Appeal.

The item(s) checked below are appropriate:

[X]	Fee for filing Appeal Brief is enclosed.	
	[X]	$250.00 - Small Entity status has been previously established in this case.
	[ ]	$500.00.
	[ ]	Not required (fee paid in prior appeal).
[ ]	Our firm's check in the amount of $_____ is enclosed.	
[X]	The Commissioner is hereby authorized to charge and/or credit Deposit Account No. 50-1017 for the following items: [X] Appeal Brief fee in the amount of **$250.00**. [X] Any overpayments or deficiencies in the above-calculated fee.	

Respectively submitted,

Adam R. Schran *et al.*

January 31, 2007 By: Clark Jablon
(Date)

CLARK A. JABLON
Registration No. 35,039
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Adam R. Schran		:	
Conf. No.:	3079	:	Group Art Unit: 2161
Appln. No.:	09/820,054	:	Examiner: Etienne Pierre Leroux
Filing Date:	March 28, 2001	:	Attorney Docket No.: 10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA		

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed on August 7, 2006 in this case.

The fees required under § 41.20 are dealt with in the accompanying "Transmittal of Appeal Brief."

I. REAL PARTY IN INTEREST

This application is assigned to Ascentive LLC, by an Assignment recorded on March 28, 2001, at Reel No. 011662, Frame 0557. Accordingly, Ascentive LLC is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants, their Assignee and their legal representatives are unaware of the existence of any related appeals and/or interferences that will directly affect, be directly affected by, or have a bearing on the decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-30 are pending in the instant application on appeal.

Claims 1-30 stand twice rejected as discussed below and are the subject of the instant appeal. The grounds of rejection in the Final Office Action dated November 21, 2006 were unclear. Accordingly, Applicants' undersigned representative telephoned the Examiner on December 7, 2006 to request clarification of the grounds. The Examiner stated that the § 102(e) rejection over U.S. Patent Application Publication No. 2002/0055912 (Buck) was withdrawn, and that the only outstanding rejection is based on Walker et al. in view of Shrader, and Walker et al. in view of Shrader and Julien Jay (Norton Internet Security 2000). The Examiner further stated that all pending claims are rejected over this combination of references, even though the grounds of rejection on page 2 of the Office Action only refers to claims 1, 2 and 4-6.

The complete text of claims 1-30, as pending, is attached hereto in Appendix VIII.

IV. STATUS OF AMENDMENTS

No amendments were filed in the present application subsequent to the Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following summary describes one preferred embodiment of the present invention. The scope of the present invention is not limited to the specific configuration or elements shown in the figures and described below.

Independent claim 1 recites a method of screening cookie files in a client machine (20), wherein a cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and

28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A request from a subscriber is received at a server to send a list of cookie file sources to the client machine (page 6, lines 1-4 and Fig. 1). The list of cookie file sources is then downloaded from the server to the client machine (page 6, lines 1-4 and Fig. 1). The downloaded list of cookie file sources is then used to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list (page 8, lines 15-17; page 9, lines 15-20; block 60 of Fig. 3).

Independent claim 7 recites a method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A first exception list is created that includes the identity of cookie file sources that are permitted to store cookie files in the client machine (personal trustlist 16 shown in Figs. 1, 3, 5 and 6). A cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A second exception list is created that includes the identity of cookie file sources that are not permitted to store cookie files in the client machine (personal blacklist 18 shown in Figs. 1, 3, 5 and 6). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). The master list is then modified in accordance with the first and second exception lists, wherein the composite list is the modified master list (page 5, lines 25-28; page 6, lines 8-14).

Independent claim 12 recites another method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). Cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine are deleted (page 5, lines 25-28; page 6, lines 8-14). Cookie file sources are added to the master list that correspond to one or more untrusted cookie file sources listed in the client machine (page 5, lines 25-28; page 6, lines 8-14). The composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources (page 5, lines 25-28; page 6, lines 8-14).

Independent claims 16, 22 and 27 recite article of manufacture versions of claims 1, 7 and 12, respectively. Support for the article of manufacture limitation is provided on page 10,

lines 20-24.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 4-17 and 18-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker et al. (hereafter, "Walker") in view of Shrader.

Claims 3 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker in view of Shrader and Julien Jay (Norton Internet Security 2000).

As discussed above, the Examiner clarified that all pending claims are rejected over these combinations of references, even though the grounds of rejection on page 2 of the Office Action only refers to claims 1, 2 and 4-6.

VIID. ARGUMENTS – REJECTIONS UNDER 35 U.S.C. § 103

A. There is a clear error in the Examiner's Final Rejection of claims 1-30 because Walker and Shrader, either taken individually, or in combination, do not disclose or suggest any of steps (a)-(c) of claims 1 and 16, at least step (c) of claims 7 and 22, and at least step (a) of claims 12 and 27

i. Background to Applicants' Invention

The following text portion from page 2, lines 19-30 of the present specification highlights one of the deficiencies in the prior art that the presently claimed invention addresses:

> There are software programs that let users create a profile of which types of cookie files they will accept. However, there is no guarantee that cookie files generated by companies with a history of abusing the use of cookie files will be screened out, nor is there a universal reference source for determining which cookie file sources should not be accepted. What is needed is a professional service that constantly researches and evaluates cookie file sources (e.g., websites), cookie files, consumer complaints and other statistical data, and develops and electronically distributes to subscribing computer users, on a periodic basis, a list of those cookie file sources that the service recommends should not be permitted to store cookie files in the subscribing user's computer. What is also needed is a user-friendly interface for enabling a user to easily and automatically modify the distributed list once it is received by the user's computer, such that the user may customize the list to meet his or her individual or organizational requirements.

Claims 1 and 7 are directed to the broad process for screening cookie files in a client machine by using a list of cookie file sources that is maintained by a server (e.g., the professional service referred to above that maintains a universal reference source) and downloaded to the client machine. Claims 7, 12, 22 and 27 are directed to a process for user editing of the list. Neither of the applied references disclose or suggest either of these claimed processes.

ii. Walker

Walker discloses a browser that is capable of accessing only web pages previously authorized by a parent or supervisor of a user of the browser. In a supervisor mode of operation, a parent can browse through any accessible web site and continually add approved web sites to a database of authorized web sites. Later, in a user mode of operation, the child is capable of accessing only those web sites that have been added to the authorized web site database. As described on column 11, lines 25-36 of Walker, the database of authorized web sites may be pre-populated with an initial pre-approved list of child-appropriate URL's that are downloaded from a remote server. The parent can then manually add more web sites to the list.

Numerous other previously applied references disclose downloading lists of child-safe websites. See, for example, the Norton Internet Security 2000 ("NIS 2000") Black web site list discussed on page 3 of the Response filed April 11, 2006 (mail date of April 6, 2006). As previously argued, this is not Applicants' invention because a list of web sites is not a list of cookie file sources. In fact, a list of web sites might not include any cookie file sources. Furthermore, the purpose of downloading a list of web sites is different than the purpose of downloading a list of cookie file sources. The purpose of downloading a list of web sites, as described in Walker or NIS 2000 is to allow users to block access to such sites. The purpose of downloading a list of cookie file sources, in one preferred embodiment of the present invention, is to prevent certain cookie files from becoming stored on a user machine, or to delete such cookie files if they were previously stored. Access to the website associated with the cookie file is not necessarily blocked.

In the Final Rejection, the Examiner states that Walker discloses a client machine that requests a "list of sources" and a server that downloads a "list of sources" to the client machine. Throughout the entire prosecution history of this patent application, which has included seven Office Actions and a myriad of different prior art rejections, no prior art reference has been cited

that discloses or suggests any of steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. In the Final Rejection, the Examiner admits that Walker does not disclose downloading a list of cookie file sources and relies instead upon Shrader for this limitation. However, as discussed below, Shrader also does not disclose downloading a list of cookie file sources, or steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. Shrader thus fails to make up for the deficiencies in Walker and its equivalent prior art references.

iii. Shrader

Shrader discloses an improved cookie control process. Column 1, line 33 through column 2, line 19 of Shrader describes the problem in the art that is addressed, and reads as follows:

> A web browser automatically stores certain user data during the process of the user browsing the Internet...
>
> Another type of user data is a so-called "cookie." Because HTTP is a stateless protocol, a cookie can be set by a server to customize data to a particular user's web browser. Cookies thus provide a degree of "state" to HTTP. By default, a browser automatically stores cookie data without giving the user the option or knowledge of it being done. When a cookie is set as part of a HTTP transaction, it will include the path the cookie is valid for, the cookie's name and value, and other optional attributes, such as the expiration date for the cookie. In the prior art, a user can configure his or her web browser to show the cookie that the web server is attempting to set in a dialog box along with the options to set or cancel the cookie. After this initial display, the cookie value is unavailable for viewing or modification by the user. The browser may store cookie values in a text file, but this file can only be viewed outside of the browser and may only be updated when the browser is closed.
>
> Thus, like basic authentication data, cookie data typically is not exposed to the user. Thus, for example, after a user has agreed to accept cookies, there is no easy way for the user to modify the cookie without first bringing down the browser.
>
> It would be highly desirable to provide a web browser user with more control over what authentication and cookie data is stored on his or her behalf by a web browser or any other HTTP client application. The present invention addresses this problem.

Shrader provides a "cookie data display routine" to address this problem, as summarized on column 2, lines 48-67, which reads as follows (underlining added for emphasis):

> The cookie display routine displays cookie data that is sent to the web browser from a given web server. The display routine places a cookie icon as part of the text and icons that remain visible above the web browser frame. The web browser displays a no-cookie icon if no cookies are set for the path. When the user selects the cookie icon, the browser displays a dialog box showing all the stored cookie values for the URL or path. A display in the dialog box shows the attributes of each cookie and scroll bars may be used to let the user browse all the values. Buttons at the bottom of the dialog box allow the user to delete or modify an existing cookie value. If desired, the cookie display routine could allow additional cookie values to be set. In addition, the cookie display routine could allow the user to view, edit, or delete all cookie values, not just ones for the current URL.
>
> <u>The cookie data display routine also enables a user to block all cookies from a particular site, such as a web server that returns nothing but advertisement graphics to subscribing URLs.</u>

Shrader's cookie data display routine is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser. That is, Shrader's routine is initiated during a normal web surfing session and not as part of a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving at a client machine a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). While Shrader arguably discloses "cookie file source(s)" in column 2, lines 64-67 as highlighted by the Examiner at the bottom of page 2 of the Final Rejection, and as underlined above, this reference to cookie file sources has nothing whatsoever to do with a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). Accordingly, one cannot simply swap out Walker's downloaded list of URL's for Shrader's cookie file sources as asserted in the Final Rejection because Shrader's cookie file sources are not downloaded in the same manner or for the same purpose as Walker's list of URL's.

In the Final Rejection, the Examiner also highlights column 7, lines 10-15 and 30-35 of Shrader, as well as the Cookie Table referred to in Fig. 7, step 405 of Shrader. However, these portions of Shrader merely confirm that Shrader's cookie control process is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser, and that Shrader's cookie control process has nothing whatsoever to do with a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27).

Referring to Fig. 7 of Shrader, the first two steps are as follows:

1. Step 400: Wait for user input
2. Step 403: Decide if user is attempting to retrieve a URL with the web browser.

These steps clearly confirm that the subsequent steps, including step 405, occur only when a user is surfing the web.

Furthermore, Shrader's scheme fails to address one of the purposes of Applicants' invention, as highlighted on page 2, lines 19-30 of the present specification (excerpted above) namely, to screen cookie files in a client machine by using a list of cookie file sources that is maintained by a server and downloaded to the client machine (claims 1 and 16), and to allow for user editing of the list (claims 7, 12, 22 and 27). Schrader's scheme requires the user to be responsible for cookie management by making all of the decisions regarding which cookie files should be blocked and which cookie files should be allowed. For example, in step 407 of Fig. 7 in Shrader, if a user tags a cookie to be blocked, the browser will not send the cookie back to the web site, thereby disrupting the process that the cookie is meant to control. One of the purposes of the present invention is to allow a service provider to provide the bulk of cookie management with the user optionally assisting in the process via a personal trustlist and personal blacklist. Shrader does not disclose or suggest any such arrangement. Instead, Shrader puts the burden of cookie management on users, most of whom have no sophisticated knowledge base to draw upon for making sound decisions regarding cookie management.

Since steps (a) and (b) of claims 1 and 16 are not disclosed or suggested by the applied combination, step (c) of claims 1 and 16 inherently cannot be met by the applied combination.

iv. Walker in view of Shrader

Shrader is directed to a completely different problem in the art as Walker. However, Shrader and Walker appear to be compatible references. The combination of Walker and Shrader would provide a web site blocking tool that would also allow a user to provide enhanced cookie control for the web sites that are not blocked by Walker's process. Such a combination, however, would still not disclose or suggest the claimed invention.

B. Summary of claim limitations that are not disclosed or suggested by Walker in view of Shrader, or Walker in view Shrader and NIS 2000

For at least the reasons discussed above, none of the references applied against the independent claims disclose or suggest at least the following underlined limitations:

> 1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:
> (a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;
> (b) downloading the list of cookie file sources from the server to the client machine; and
> (c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.
>
> 7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:
> (a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;
> (b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;
> (c) receiving at the client machine, from a service provider, a master list of cookie file sources; and
> (d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.
>
> 12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:
> (a) receiving at the client machine, from a service provider, a master list of cookie file sources;
> (b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;
(b) downloading the list of cookie file sources from the server to the client machine; and
(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;
(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

Furthermore, the unique combination of steps (a)-(c) in claims 1 and 16; steps (a)-(d) in claims 7 and 22; and steps (a)-(c) in claims 12 and 27 are not disclosed or suggested by the applied references.

In view of the above remarks, claims 1, 7, 12, 16, 22 and 27 are believed to be patentable over Walker in view of Shrader.

C. Patentability of dependent claims

The dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

Regarding dependent claims 3 and 18, NIS 2000 does not make up for any of the above-highlighted deficiencies in Walker or Schrader.

D. Applicants' arguments do not stand or fall based on application of the CAFC's nonobviousness doctrine using a motivation/suggestion/teaching test

According to this CAFC test, when various pieces of prior art each contain elements of an invention, the prior art can be combined together to invalidate a patent on the invention only when there is some motivation, suggestion, or teaching to combine the prior art. The U.S. Supreme Court has granted a *writ of certiorari* in KSR International Co. v. Teleflex Inc. (Fed. Cir. 2006) to decide if the CAFC's motivation/suggestion/teaching test is legally correct in view of Supreme Court precedent. Commentators expect the Supreme Court to decide if the CAFC test is consistent with the Supreme Court's test in Sakraida v. Ag Pro, Inc. 425 U.S. 273 (1976). In Sakraida, the arrangement of old elements with each performing the same function it had been known to perform in the prior art was deemed to be not patentable, even though the novel arrangement perhaps produces a more striking result than in previous combinations. Sakraida is considered to be a case where patentability of a new combination was denied, even though there was no explicit motivation, suggestion, or teaching to combine the old elements.

Here, patentability of the claimed invention does not rely solely upon the motivation/suggestion/teaching test because the combination of references still lacks any disclosure of at least steps (a) and (b) of claims 1 and 16, step (c) of claims 7 and 22, and step (a) of claims 12 and 27. Accordingly, these claims are believed to be patentable even under the

Supreme Court's test in Sakraida, and regardless of whether the Supreme Court repudiates the CAFC's motivation/suggestion/teaching test.

E. Conclusion

For the reasons set forth above, Appellants respectfully submit that pending claims 1-30 are patentable over the prior art applied by the Examiner. Reversal of the rejections and issuance of a Notice of Allowance are respectfully requested at the earliest opportunity.

VIII. APPENDIX OF CLAIMS

1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

2. The method of claim 1, further comprising:

(d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;

(e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and

(f) modifying the downloaded list in accordance with the first and second exception lists.

3. The method of claim 1, further comprising:

(d) receiving updates of the downloaded list from the server on a periodic basis.

4. The method of claim 1, further comprising:

(d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

5. The method of claim 1, further comprising:

(d) removing detected cookie files stored in the client machine.

6. The method of claim 1, further comprising:

(d) preventing detected cookie files from being stored in the client machine.

7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

8. The method of claim 7, wherein the composite list is stored in the client machine independent of the first exception list, the second exception list and the received master list.

9. The method of claim 7, further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

10. The method of claim 7, further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

11. The method of claim 7, further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

13. The method of claim 12, wherein the master list and the composite list are stored

independently in the client machine.

14. The method of claim 12, further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

15. The method of claim 12, further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

17. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;

(e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and

(f) modifying the downloaded list in accordance with the first and second exception lists.

18. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) receiving updates of the downloaded list from the server on a periodic basis.

19. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

20. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) removing detected cookie files stored in the client machine.

21. The article of manufacture of claim 16, wherein the computer-executable instructions

perform a method further comprising:

(d) preventing detected cookie files from being stored in the client machine.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

23. The article of manufacture of claim 22, wherein the composite list is stored in client machine independent of the first exception list, the second exception list and the received master list.

24. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

25. The article of manufacture of claim 22, wherein the computer-executable instructions

perform a method further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

26. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

28. The article of manufacture of claim 27, wherein the master list and the composite list are stored independently in the client machine.

29. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

30. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

IX. APPENDIX OF EVIDENCE

No evidence has been included.

X. APPENDIX OF RELATED DECISIONS

None.

XI. OTHER MATERIAL THAT APPELLANT CONSIDERS NECESSARY OR DESIRABLE

See the accompanying Supplemental Information Disclosure Statement that includes a citation for U.S. Patent No. 5,706,507 (Schloss).

During the telephone conversation of December 7, 2006, the Examiner stated that he located an additional reference (Schloss) after issuing the Final Rejection that he believes should be formally applied against the claims. Applicants have carefully reviewed Schloss and do not believe that it is any more relevant to the presently claimed invention than the current prior art of record. Schloss does not disclose any of the above-highlighted (underlined) limitations in the independent claims.

Respectively submitted,

Adam R. Schran *et al.*

January 31, 2007 By: Clark Jablon
(Date)

CLARK A. JABLON
Registration No. 35,039
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1293